CLAIMS

What is claimed is:

1. A method for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network, the method comprising:
the peer node generating a secured communication request to the intermediary peer node;
the intermediary peer node authenticating the peer node in response to said secured communication request, and
the intermediary peer node issuing a signed certificate of authority upon successful authentication.

2. The method of claim 1 wherein said secured communication request comprises a certificate signing request, a unique identifier, and a password.

3. The method of claim 2 wherein said certificate signing request includes a public key cryptography system (PKCS) certificate signing request.

4. The method of claim 1 wherein said secured communication protocol comprises a transport layer data authentication protocol.

5. The method of claim 1 wherein said intermediate peer node is communicatively coupled to an enterprise database, said enterprise database authenticates the peer node in response to said secured communication request.

6. The method of claim 1 further comprising securing a pipe connection between the peer node and the intermediary peer node upon authentication.

7. The method of claim 6 further comprising closing said pipe connection upon failed authentication of said node.

8. The method of claim 1 wherein said peer node comprises a peer node advertisement and a pipe node advertisement.

9. The method of claim 8 wherein said peer node advertisement comprises a peer node name, a unique peer node identifier, and local transport information.

10. The method of claim 8 wherein said pipe node advertisement includes an application-dependent port identifier, said unique identifier, a name, and a type.

11. The method of claim 1 wherein the peer-to-peer network operates using a JXTA technology-enabled platform.

12. A method for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network, the method comprising:

generating a secured communication request to the intermediary peer node capable of authenticating the peer node in response to said secured communication request, and

receiving a signed certificate of authority upon successful authentication.

13. The method of claim 12 wherein said secured communication request comprises a certificate signing request, a unique identifier, and a password.

14. The method of claim 13 wherein said certificate signing request includes a public key cryptography system (PKCS) certificate signing request.

15. The method of claim 12 wherein said secured communication protocol comprises a transport layer data authentication protocol.

16. The method of claim 12 wherein said intermediate peer node is communicatively coupled to an enterprise database, said enterprise database authenticates the peer node in response to said secured communication request.

17. The method of claim 12 further comprising securing a pipe connection between the peer node and the intermediary peer node upon authentication.

18. The method of claim 17 further comprising closing said pipe connection upon failed authentication of said node.

19. The method of claim 12 wherein said peer node comprises a peer node advertisement and a pipe node advertisement.

20. The method of claim 19 wherein said peer node advertisement comprises a peer node name, a unique peer node identifier, and local transport information.

21. The method of claim 19 wherein said pipe node advertisement includes an application-dependent port identifier, said unique identifier, a name, and a type.

22. The method of claim 12 wherein the peer-to-peer network operates using a JXTA technology-enabled platform.

23. A method for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network, the method comprising:

receiving a secured communication request from the peer node;

authenticating the peer node in response to said secured communication request; and

sending a singed certificate of authority upon successful authentication.

24. The method of claim 23 wherein said secured communication request comprises a certificate signing request, a unique identifier, and a password.

25. The method of claim 24 wherein said certificate signing request includes a public key cryptography system (PKCS) certificate signing request.

26. The method of claim 23 wherein said secured communication protocol comprises a transport layer data authentication protocol.

27. The method of claim 23 wherein said intermediate peer node is communicatively coupled to an enterprise database, said enterprise database authenticates the peer node in response to said secured communication request.

28. The method of claim 23 further comprising securing a pipe connection between the peer node and the intermediary peer node upon authentication.

29. The method of claim 28 further comprising closing said pipe connection upon failed authentication of said node.

30. The method of claim 23 wherein said peer node comprises a peer node advertisement and a pipe node advertisement.

31. The method of claim 30 wherein said peer node advertisement comprises a peer node name, a unique peer node identifier, and local transport information.

32. The method of claim 30 wherein said pipe node advertisement includes an application-dependent port identifier, said unique identifier, a name, and a type.

33. The method of claim 23 wherein the peer-to-peer network operates using a JXTA technology-enabled platform.

34. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network, the method including:

the peer node generating a secured communication request to the intermediary peer node;

the intermediary peer node authenticating the peer node in response to said secured communication request, and

the intermediary peer node issuing a signed certificate of authority upon successful authentication.

35. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for administrating peer-to-peer networks, the method including:

generating a secured communication request to the intermediary peer node capable of authenticating the peer node in response to said secured communication request, and

receiving a signed certificate of authority upon successful authentication.

36. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for administrating peer-to-peer networks, the method including:

receiving a secured communication request from the peer node;

authenticating the peer node in response to said secured communication request; and

sending a signed certificate of authority upon successful authentication.

37. An apparatus for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network comprising:

means for generating a secured communication request to the intermediary peer node;

means for authenticating the peer node in response to said secured communication request, and

means for issuing a signed certificate of authority upon successful authentication.

38. An apparatus for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network comprising:

means for generating a secured communication request to the intermediary peer node capable of authenticating the peer node in response to said secured communication request, and

means for receiving a signed certificate of authority upon successful authentication.

39. An apparatus for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network comprising:

means for receiving a secured communication request from the peer node;

means for authenticating the peer node in response to said secured communication request; and

means for sending a signed certificate of authority upon successful authentication.

40. A peer-to-peer network system comprising:

a peer node;

an intermediary peer node communicatively coupled to said peer node;

wherein said peer node is configured to generate a secured communication request to said intermediary peer node;

wherein said intermediary peer node is configured to authenticate said peer node in response to said secured communication request, and

wherein said intermediary peer node is configured to issue a signed certificate of authority upon successful authentication,

41. A peer node comprising:

a processor; and

a memory comprising program instructions, wherein the program instructions are executable by the processor to:

generate a secured communication request to the intermediary peer node capable of authenticating the peer node in response to said secured communication request, and

receive a signed certificate of authority upon successful authentication.

42. An intermediary peer node comprising:

a processor; and

a memory comprising program instructions, wherein the program instructions are executable by the processor to:

receive a secured communication request from the peer node;

authenticate the peer node in response to said secured communication request; and

send a signed certificate of authority upon successful authentication.